Amendments to the Claims:

Amendments to the claims are reflected in the following listing, which replaces any and all prior versions and listings of claims in the present application:

Claim Listing

1. (Currently Amended) A smartcard transaction system configured with a biometric security device, said system comprising:

a smartcard configured to communicate with a reader, wherein said reader and said biometric security device are configured to communicate with a host ~~said system~~;

an integrated circuit device disposed within said smartcard and configured to communicate with said reader, said integrated circuit device comprising a common application and a second application, said second application being configured to store travel-related information associated with a cardholder;

said second application comprising a common file structure and a partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to a field in said common file structure;

said biometric security device comprising a biometric sensor configured to communicate with said system and detect a first proffered biometric sample and a second proffered biometric sample, wherein said first proffered biometric sample is a different type of biometric sample ~~and~~ from said second proffered biometric sample, and wherein said first proffered biometric sample and said second proffered biometric sample are from the same person ~~include different biometric data~~, and wherein said first proffered biometric sample is required to access said common file structure and said second proffered biometric sample is required to access said partner file structure; and,

a verification device configured to verify said first proffered biometric sample to facilitate access to said common file structure and configured to verify said second proffered biometric sample to facilitate access to said partner file structure;

wherein upon verification by said verification device, said common application is configured to transfer common data to facilitate said transaction, and said second application is configured to transfer said travel-related information, information related to said common file structure and information related to said partner file structure to facilitate said transaction.

a smellprint sensor configured to detect a proffered smellprint sample to generate data representing said proffered smellprint sample, said smellprint sensor configured to communicate with said system, wherein at least one of said first proffered biometric sample and said second proffered biometric sample includes said proffered smellprint sample; ~~said system configured to use said data representing said proffered smellprint sample as a variable in an encryption calculation to secure at least one of user data and transaction data~~; and,

a device configured to verify said proffered smellprint sample to facilitate a transaction .

2. (Original) The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

3. (Currently Amended) The smartcard transaction system of claim 1, wherein said system is configured to use ~~said~~ data representing said proffered smellprint sample as a message authentication code, as a variable in an encryption calculation and as at least one of a private key and a public key to facilitate encryption security associated with said transaction.

4. (Currently Amended) The smartcard transaction system of claim 1, wherein said system is configured to use ~~said~~ data representing said proffered smellprint sample in generating a message authentication code .

5. (Original) The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered smellprint samples, proffered and registered user information, terrorist information, and criminal information.

6. (Original) The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

7. (Currently Amended) The smartcard transaction system of claim 1 ~~7~~ , ~~further comprising an integrated circuit device disposed within said smartcard and configured to communicate with said reader, said integrated circuit device comprising a common application and a second application, said~~

~~second application being configured to store travel-related information associated with a cardholder; and~~

~~said second application comprising a common file structure and a partner file structure, wherein said partner file structure provides write access to a field within said partner file structure for a first partnering organization and denies write access to said field for a second partnering organization, and said common file structure provides write access for said first partnering organization and said second partnering organization to file in said common file structure;~~

said first partner file structure configured to store card-holder preferences relating to at least one of rental cars, hotel reservations, and air travel

~~said partner file structure further configured to enable said first partnering organization to program said smartcard as a room key~~.

8. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor device is configured with at least one of an electronic sensor, chemical sensor, gas chromatograph, spectrometer, conductivity sensor and piezoelectric sensor.

9. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor is configured to detect and verify smellprint characteristics using at least one of statistical, ANN and neuromorphic techniques.

10. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor is configured to detect and verify smellprint characteristics including molecular structures, chemical compounds, temperature, mass differences, pressure, force and odorants.

11. (Original) The smartcard transaction system of claim 1, wherein said smellprint sensor device is configured to detect false odorants, man-made smells, abnormal odorants and body heat.

12. (Original) The smartcard transaction system of claim 1, further including a device configured to compare a proffered smellprint sample with a stored smellprint sample.

13. (Original) The smartcard transaction system of claim 12, wherein said device configured to compare a smellprint sample is at least one of a third-party security vendor device and local CPU.

14. (Original) The smartcard transaction system of claim 12, wherein a stored smellprint sample comprises a registered smellprint sample.

15. (Original) The smartcard transaction system of claim 14, wherein said registered smellprint sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

16. (Original) The smartcard transaction system of claim 15, wherein different registered smellprint samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

17. (Original) The smartcard transaction system of claim 15, wherein a smellprint sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a smellprint sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

18. (Original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered smellprint sample.

19. (Original) The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered smellprint sample.

Claim 20 (Cancelled).

21. (Currently Amended) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods .

22. (Original) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

23. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system having a biometric security device, said method comprising:

communicating with a smartcard, wherein said smart card comprises a common application and a second application, said second application storing travel-related information associated with a cardholder, said second application comprising a common file structure and a partner file structure;

receiving a first proffered biometric sample and a second proffered biometric sample, wherein said first proffered biometric sample is ~~proffering a smellprint to a smellprint sensor communicating with said system to initiate verification of~~ a smellprint sample for facilitating authorization of ~~a~~ said smartcard transaction;

generating data representing said ~~proffered~~ smellprint sample;

wherein said first proffered biometric sample is a different type of biometric sample from said second proffered biometric sample, and wherein said first proffered biometric sample and said second proffered biometric sample are from the same user, and wherein said first proffered biometric sample is required to access said common file structure and said second proffered biometric sample is required to access said partner file structure;

verifying said first proffered biometric sample and a second proffered biometric sample;

enabling write access to a field within said partner file structure upon verification of said second proffered biometric sample and upon request by a first partnering organization;

denying write access to said field upon request by a second partnering organization;

enabling write access for said first partnering organization and said second partnering organization to a field in said common file structure, upon verification of said first proffered biometric sample;

transferring common data to facilitate said smartcard transaction; and,

transferring said travel-related information, information related to said common file structure and information related to said partner file structure to facilitate said smartcard transaction.

~~; and~~

~~using said data representing said proffered smellprint sample as a variable in an encryption calculation to secure at least one of user data and transaction data. .~~

24. (Original) The method for of claim 23, further comprising registering at least one smellprint sample with an authorized sample receiver.

25. (Original) The method of claim 24, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a smellprint to said authorized sample receiver, processing said smellprint to obtain a smellprint sample, associating said smellprint sample with user information, verifying said smellprint sample, and storing said smellprint sample upon verification.

26. (Currently Amended) The method of claim 23, wherein said receiving step comprises receiving ~~of proffering includes proffering~~ a smellprint at ~~to~~ at least one of an electronic sensor, chemical sensor, gas chromatograph, spectrometer, conductivity sensor and piezoelectric sensor.

Claim 27 (Cancelled).

28. (Previously Presented) The method of claim 23, further comprising using said data representing said proffered smellprint sample as at least one of a private key, a public key, and a message authentication code to facilitate transaction security measures .

29. (Previously Presented) The method of claim 23, further comprising using said data representing said proffered smellprint sample in generating a message authentication code and as at least one of a private key and a public key wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes comparing a proffered smellprint sample with a stored smellprint sample.

30. (Currently Amended) The method of claim 23 , ~~wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification~~ further ~~includes~~ comprising

comparing ~~a proffered~~ said smellprint sample to a stored smellprint sample by using at least one of a third-party security vendor device and local CPU.

31. (Previously Presented) The method of claim 30 , wherein said step of comparing includes comparing smellprint characteristics using at least one of statistical, ANN and neuromorphic techniques.

32. (Currently Amended) The method of claim 23, ~~wherein said step of proffering a smellprint to a smellprint sensor communicating with said system~~ further comprises using ~~said~~ a smellprint sensor to detect at least one of false odorants, man-made smells, abnormal odorants and body heat.

33. (Currently Amended) The method of claim 23, further comprising using said data representing said ~~proffered~~ smellprint sample to facilitate substantially simultaneous access to goods and initiation of authentication for a subsequent purchase of said goods .

34. (Currently Amended) The method of claim 23, ~~wherein said step of proffering a smellprint to a smellprint sensor communicating with said system to initiate verification further includes the use of at least one~~ further comprising using a secondary security procedure.

Claims 35-47 (Cancelled).

48. (New) The smartcard transaction system of claim 1, further comprising:

a first enterprise data collection unit associated with a first enterprise, said first enterprise data collection unit configured to store update transactions and pending transactions associated with said smartcard and said first enterprise;

a second enterprise data collection unit associated with a second enterprise, said second enterprise data collection unit configured to store update transactions and pending transactions associated with said smartcard and said second enterprise;

at least one access point configured to interface with said smartcard and said first and second enterprise data collection units;

a card object database system coupled to said first and second enterprise data collection units and configured to store said smartcard information in accordance with said update transactions and

said pending transactions, wherein said smartcard information includes a card object having at least one application;

an update logic system configured to route said smartcard information from said first and second enterprise data collection units to said at least one access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

wherein said verification device activates said update logic system upon verification of said first proffered biometric sample and said second biometric sample.

49. (New) The smartcard transaction system of claim 48, further comprising an update logic system coupled to at least one enterprise data synchronization interface, said update logic system configured to securely route card information between said enterprise data synchronization interface and said enterprise data collection units, said enterprise data synchronization interface coupled to an enterprise network configured to communicate with said access point.

50. (New) The smartcard transaction system of claim 49, further comprising a secure support client server configured to communicate with said access point, said secure support client server further configured to adaptively provide communication functionality in accordance with the communication functionality available at said access point.

51. (New) The smartcard transaction system of claim 50, further including a personalization system comprising:

a security server;

at least one key system associated with said at least one application, said key system configured to communicate with said security server and to supply a key in response to a request from said security server;

a personalization utility configured to receive said card object and to communicate with said security server;

said personalization utility further configured to add said key to said card object, a card management system, said card management system configured to accept a card request and communicate said card request to said personalization utility; and

a gather application module configured to communicate with said card management system and gather application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

52. (New) The smartcard transaction system of claim 1, wherein said first proffered biometric sample is associated with a first plurality of financial accounts and a first set of rules related to said transaction, and said second biometric sample is associated with a second plurality of financial accounts and a second set of rules related to said transaction, wherein said first plurality of financial accounts include different financial accounts than said second plurality of financial accounts.